Top 5 Cyber-Defense Practices for 9-1-1

Prepared by the APCO Cybersecurity Committee

As we start thinking about goals for the new year, cyber defense should be a top priority for our Emergency Communication Centers (ECC). This past year we've seen an increasing number of cyberattacks targeting our industry. When we are not prepared for these attacks, they can threaten our critical services, cause the loss of evidence and other data, as well as cost us money and time that we can't afford. To help plan for the new year, we've accumulated a list of top cyber-defense practices that ECC's across the US have used to successfully defend against and recover from cyberattacks.

1. **Plan:** At this time, it's not a matter about "if", but "when" you will be impacted by a cyber attack. All 50 states have reported cyberattacks impacting local governments and 9-1-1 in the last 2 years. Having a cyber incident response plan that is accessible and known to your staff during a crisis is critical to effective response and recovery. Many trusted organizations and institutions have guidelines for creating incident response plans. However, a plan is only useful if it can be executed properly.
2. **Train:** Your people are the first line of defense against cyber attacks and scams that feed on tricking people, like phishing emails. All staff have email accounts and access to internet-connected technology. Training all personnel on the basics of cyber hygiene can make you up to 40% safer. Noticing suspicious activity and reporting it early can be the difference between one infected computer vs. an entire department's system being locked down.
3. **Patch:** Sophisticated cyber attacks can be rented from the dark web easily and cheaply, and many cast a wide net looking for victims by searching for known vulnerabilities. The vast majority of these attacks are not zero-day events and can be thwarted by patching outdated software. By staying on top of new security updates for your systems and making sure that your venders do the same, you can prevent many attacks.
4. **Backup:** When you are hit with ransomware that locks up your systems or malware that deletes data, having backups can save you from negotiating with a criminal or losing critical digital files, like evidence. A 3-2-1 backup strategy is a well-known best practice. This means having 3 backups at all times, 2 local but on different devices, and 1 off-site.
5. **Monitor**: Two important steps in mitigating a cyber attack are discovering that there has been an incident and identifying the infiltration method. Continuously monitoring the cyber behavior in your system and the data flowing between you and the outside world is invaluable in this process. The faster you can discover a problem, the sooner you can isolate it and prevent it from spreading. Knowing what data has been communicated and how it was communicated is the key to closing the door on future attacks.

It’s impossible to remove all risk of attack; however, following these five best practices is a great step towards increasing our 9-1-1 centers’ cyber-defense and protecting our critical services to the public.